

REMARKS/ARGUMENTS

Claims 1-25 are pending in this application. The Office Action has been reviewed. Favorable reconsideration is respectfully requested.

Applicant notes with appreciation the indication that claims 7-10 and 19-22 are allowable over the prior art of record.

By this Amendment, Claims 11, 12, 23 and 24 are amended to address the rejection under 35 U.S.C. 112, second paragraph (see page 2 of the Office Action). Other minor amendments to the claims have been made to correct typographical errors. Applicant respectfully submits that these minor claim amendments do not materially affect the scope of the claims.

On page 3 of the Office Action, the Examiner rejected Claims 1-6, 11-18, 24 and 25 under U.S.C. 103(a) as being unpatentable over U.S. Patent 6,035,041 granted to Frankel et al. and further in view of U.S. Patent 6,185,678 granted to Arbaugh et al. This rejection is respectfully traversed.

Before turning to the Examiner's rejection on the merits, a brief overview of the cited prior art and the

embodiments of the invention (embraced by Claim 1) would assist in understanding the distinguishing features of the invention over the prior art.

U.S. Patent 6,035,041 (Frankel et al.) discloses that:

Proactive robust threshold schemes are presented for general 'homomorphic-type' public key systems, as well as optimized systems for the RSA function. Proactive security employs dynamic memory refreshing and enables us to tolerate a 'mobile adversary' that dynamically corrupts the components of the system (perhaps all of them) as long as the number of corruptions (faults) is bounded within a time period. The systems are optimal-resilience. Namely they withstand any corruption of minority of servers at any time-period by an active (malicious) adversary i.e., any subset less than half. Also disclosed are general optimal-resilience public key systems which are 'robust threshold' schemes (against stationary adversary), and are extended to 'proactive' systems (against the mobile one). The added advantage of proactivization in practical situations is the fact that, in a long-lived threshold system, an adversary has a long time (e.g., years) to break into any t out of the l servers. In contrast, the adversary in a proactive systems has only a short period of time (e.g., a week) to break into any t servers. The model of mobile adversary seems to be crucial to such 'long-lived' systems that are expected to span the secure network and electronic commerce infrastructure. (Abstract)

Frankel's purpose is, *inter alia*, to extend protection from stationary adversary to 'proactive' systems (against the mobile adversary). The added advantage of proactivization in practical situations is the fact that, in a long-lived threshold system, an adversary has a long time (e.g., years) to break into any t out of the l servers. In

contrast, the adversary in a proactive systems has only a short period of time (e.g., a week) to break into any t servers.

Frankel assumes that the information received from mating servers during renewal/recovery procedure is trusted and/or authenticated and this is a significant mitigating circumstance for applying Frankel's protocol. This can be learned, *inter alia*, from the fact that for Frankel's protocol it is not material whether the procedure is renewal or recovery (see column 11, lines 33-34). Had Frankel been concerned with authenticity/trust of the messages exchanged during the protocol, this would render the recovery process considerably more difficult than the renewal process.

If the specified mitigating circumstance does not apply, Frankel's protocol could be applied using e.g. a technique disclosed in reference no. 3 (that is referred to in the present application) - see page 19, lines 13-18 - by having other servers keep in read-only ROM memory a copy of the non-proactive related key V_{CERT} to guarantee authenticity of message received during the protocol. However, holding V_{CERT} in a ROM of every server is an inherent limitation as described in detail on page 19, line 18 to page 20, line 2 of the present application.

In accordance with a certain embodiments of Claim 1 of the invention, the need to store explicitly V_{CERT} in every server is obviated and restoration of the latter is achieved on the basis of V_{start}^I (which for example can be stored on the ROM of the computer during manufacturing time and is unique and not group related) and "restore related information" that is generated during initialization procedure.

Having restored V_{CERT} then, for instance, the procedure described in Ref. 3 of the patent application can be invoked for guaranteeing trusted/authenticated messages exchanged in Frankel's protocol thereby achieving the enhanced procedure of the kind described in Frankel. In other words, Frankel's protocol can be applied without assuming trusted/authenticated exchanged messages and without requiring each participating server to store V_{CERT} . It should be noted that the procedure described above for realizing the embodiment of Claim 1 in conjunction with Ref. 3 and Frankel are provided for illustrative purposes only and is, of course, not binding.

Bearing this in mind attention is now drawn to the Examiner's comments in respect of Claims 1, 13 and 25 in page 3 of the Office Action.

The Examiner admits that Frankel's specification fails to disclose restoring procedure using the individual server's public key information. The Examiner refers to Arbaugh et al. (U.S. Patent 6,185,678) alleging that public key information from the computer system ROM is used to restore the computing system. However, this allegation does not take into account the fact that an underlying assumption of Arbaugh et al. is that there exists a so called trusted repository (see Abstract, lines 14-15 to wit: - "...the present invention under the additional assumption of the availability of a trusted repository") which actually suggests that if certain conditions are met a verified copy of the failed component is copied from the trusted host. By analogy, this would suggest that there exists a trusted server which stores the V_{CERT} data and which can be accessed (for copying V_{CERT}) if certain criterion are met. This, in fact, teaches away from the present invention as defined in Claim 1, which, *inter alia*, aims at coping that the limitations of hitherto known systems (such as the ones described in Ref. 3), and according to Claim 1 obviates the need to store V_{CERT} and naturally does not require existence of trusted party. Thus, Claim 1 recites that V_{CERT} is restored on the basis of V_{start}^I and restore related information. Note, that from the latter limitation of Claim 1, it readily arises that there is no trusted party that stores

the V_{CERT} information. A non-limiting example how this is achieved is set forth in the first two paragraphs of page 25 of Applicant's specification.

Applicant therefore submits that, *inter alia*, the feature a restore procedure for utilizing at least said public, non proactive related, key V_{start}^I and said restore related information for restoring at least said public proactive key V_{CERT} . recited in Claim 1 is not suggested by either Frankel nor Aubaugh, which as specified above, teach away from the claimed features of Claim 1.

Moreover, Applicant respectfully submits that the Office Action does not set forth a *prima facie* case of obviousness, in that it does not show that the prior art suggests motivation to combine the references. In *In re Lee*, 61 USPQ2d 1430 (Fed Cir. 2002), the Federal Circuit held that

[w]hen patentability turns on the question of obviousness, the search for and analysis of the prior art includes evidence relevant to the finding of whether there is a teaching, motivation, or suggestion to select and combine the references relied on as evidence of obviousness.

. . . .

The "common knowledge and common sense" on which the Board relied in rejecting Lee's application are not the specialized knowledge and expertise contemplated by the Administrative Procedure Act. . . . The Board's findings must extend to all material facts and must be documented on

the record, lest the "haze of so-called expertise" acquire insulation from accountability. "Common knowledge and common sense," even if assumed to derive from the agency's expertise, do not substitute for authority when the law requires authority.

Id. at 61 USPQ2d at 1433-1434.

For at least these reasons, Applicant respectfully submits that claim 1 is patentable over the prior art, whether taken alone or in combination as proposed in the Office Action. In light of the foregoing discussion Applicant respectfully requests that the rejection of Claim 1 be withdrawn.

Claims 2-6, 11-12 dependent from Claim 1 are believed to be patentable, *inter alia*, for the reasons described with reference to Claim 1.

Claim 13 directed to a method should be deemed novel and non-obvious over the cited prior art for the reasons discussed in detail with reference to Claim 1. Claims 14-18, 23-24, dependent from Claim 13 are believed to be allowable, *inter alia*, for the reasons described with reference to Claim 13.

Claim 25 directed to a storage medium should be deemed novel and non-obvious as cited in the prior art for the reasons discussed in detail with reference to Claim 1.

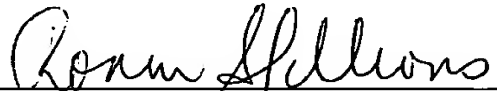
Appln. No. 09/431,067
Amdt. dated January 23, 2004
Reply to Office Action of Sept. 30, 2003

In light of the foregoing discussions,
reconsideration and withdrawal of the outstanding rejections
is respectfully requested. Applicant submits that the
application is in condition for allowance and early notice to
this effect is most earnestly solicited.

If the Examiner has any questions, he is invited to
contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By 
Ronni S. Jyllions
Registration No. 31,979

RSJ:ma
624 Ninth Street, N.W.
Washington, D.C. 20001
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\C\cohn\herzberg1\pto\Amendment-A.doc